(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 039 655 A2

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
27.09.2000 Bulletin 2000/39

(51) Int. Cl.[7]: H04B 1/713

(21) Application number: 00302259.7

(22) Date of filing: 20.03.2000

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 23.03.1999 US 125573 P
29.12.1999 US 473337

(71) Applicant:
Texas Instruments Incorporated
Dallas, Texas 75251 (US)

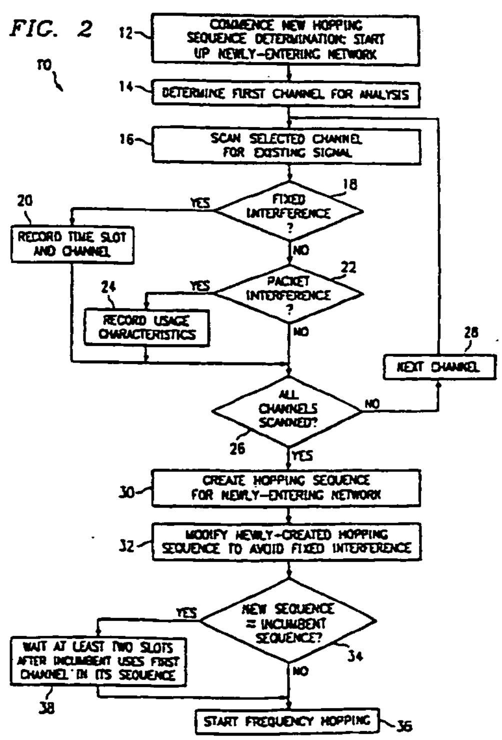
(72) Inventors:
- Panasik, Carl M.
  Garland, Texas 75044 (US)
- Siep, Thomas M.
  Garland, Texas 75040 (US)

(74) Representative:
Potter, Julian Mark
D. Young & Co.,
21 New Fetter Lane
London EC4A 1DA (GB)

(54) System and method for wireless frequency hopping network

(57) A method (10) for determining a frequency hopping sequence for a newly-entering network. The method comprises the step of scanning (16) a plurality of frequency channels. For each of the plurality of frequency channels, the scanning step comprises detecting whether a signal (18,22) exists on the channel and recording information (20,24) corresponding to each channel on which a signal is detected. Finally, and responsive to the recorded information, the method forms (30) the frequency hopping sequence.

FIG. 2



EP 1 039 655 A2

Description

[0001] The present embodiments relate to wireless communication systems and are, more particularly, but not exclusively, directed to such systems using frequency hopping.

[0002] Wireless networks are becoming increasingly popular, and in this regard there has been improvement in many aspects of such networks. Some improvements relate to configurations that permit simultaneous operation of different networks where there is minimal or no interference between communications belonging to each of the networks. In this respect, the term network is used, and is further used in the same manner for the remainder of this document, to describe a system consisting of an organized group of intercommunicating devices. Further in this respect, the different networks may be labeled according to a first network that is already transmitting in time followed by a second network in time seeking to transmit and thereby possibly communicating and causing interference due to a communication overlapping the pre-existing communication of the first network. Accordingly, to facilitate the remaining discussion, such a first network is referred to as an incumbent network, while the network which seeks to communicate, or in fact does communicate, after the incumbent network is referred to as the newly-entering network. Given this terminology, the present background and embodiments discussed below are directed to reducing interference between incumbent network communications and newly-entering network communications.

[0003] One approach to reducing the above-introduced interference is known in the art as spread spectrum frequency hopping and is sometimes referred to more simply as frequency hopping. In frequency hopping, a newly-entering network transmitter transmits packets of information at different frequencies in an effort to reduce the chance that the packet will interfere or "collide" with a packet transmitted at a frequency by a transmitter in an incumbent network. The change between frequencies, that is, from one frequency to another, is said to be a "hop" between the frequencies. Moreover, the goal is such that each packet from a newly-entering network is transmitted at a frequency which neither overlaps nor is near enough to a frequency at which an incumbent network is transmitting. Further in this regard, some systems (e.g., using Bluetooth protocol) transmit each successive packet at a different frequency, that is, the transmitter is "hopping" to a different frequency for each packet. Alternatively, others systems (e.g., IEEE 802.11) transmit a first set of packets at a first frequency, and then hop to a second frequency to transmit a second set of packets, and so forth for numerous different sets of packets at numerous different respective frequencies. Note further that if interference or a collision does occur, it typically corrupts the data of both packets, that is, the data transmitted by both the newly-entering network and the incumbent network. As a result, both networks are then required to retransmit the packets an additional time so as to replace the corrupted data resulting from the collision.

[0004] In an effort to achieve minimal packet collision using frequency hopping, two prior art methods have arisen for determining the different frequencies to which a network will hop. In a first method, a frequency hopping network uses a pre-ordained hopping sequence. This first approach is used by way of example under the IEEE 802.11 standard. In a second method, a seed is provided to a pseudo-random generator which produces a corresponding pseudo-random series of frequencies along which the network hops. This second approach is used by way of example under the fairly recently developed Bluetooth protocol. Both of these approaches have achieved some level of success in reducing the amount of inter-network packet collision. Nevertheless, the present inventors have empirically determined that by locating two or more different networks in the same vicinity such that transmissions from each different network effectively compete for airtime, there still arises a considerable amount of packet collisions, thereby reducing the effective transmission rate for each network.

[0005] Frequency hopping as described thus far reduces the chances of interference between a packet from newly-entering network and a packet from an incumbent network. Further in this regard and by way of additional background, Figure 1 illustrates communications of such packets and, as detailed below, it also illustrates instances where packet collisions occur. Looking to Figure 1 in greater detail, its horizontal axis illustrates time (or time slots), and its vertical axis indicates frequency. Additionally, Figure 1 illustrates a number of blocks, where each block is intended to depict a packet as transmitted by either an incumbent network or a newly-entering network. Further in this regard, note that the term "packet" is used in this document to define a block of information sent in a finite period of time, where subsequent such packets are sent at other times. This block of information may take on various forms, and sometimes includes different information types such as a preamble or other type of control information, followed by user information which is sometimes also referred to as user data. Further, the overall packet also may be referred to in the art by other names, such as a frame, and thus these other information blocks are also intended as included within the term "packet' for purposes of defining the present inventive scope. In any event, returning to Figure 1, for the sake of reference, each packet illustrated in Figure 1 is labeled with an identifier using the letter "P" (i.e., for packet) and following after that letter is a number corresponding to the network which transmitted the packet. More particularly, packets transmitted by the first network (i.e., the incumbent network) are labeled with an identifier P1 while packets transmitted by the second network (i.e., the

newly-entering network) are labeled with an identifier P2. Further, the subscript for each packet identifies a time period encompassed by the duration of the packet. For example, during a time t_0, the first network transmits a packet $P1_0$ while also during time t_0 the second network transmits a packet $P2_0$. Further in this regard, in the prior art transmissions by the first network are asynchronous with respect to transmissions of the second network, both in start time and periodicity. Thus, time t_0 is only meant as a relative indication for the first packet from each network, and it is not intended to suggest that the packets from both networks begin and end at the same time.

[0006] With respect to all packets in Figure 1, the preceding demonstrates that each packet begins at a certain time, ends at a later time, and fills a certain frequency range (where the range is referred to as a channel). As a result and as described below, interference may occur if the area in Figure 1 defined by a packet overlaps or is within a certain distance of a packet from another wireless link. Indeed and as discussed below, such interference may occur in one of four different ways.

[0007] Time t_1 in Figure 1 illustrates a first type of packet interference, where it may be seen that the first network transmits a packet $P1_1$. After packet $P1_1$ commences but also during time t_1 the second network transmits a packet $P2_1$. The overlap of packets $P1_1$ and $P2_1$ is shown as a first collision C_1. Note that the horizontal alignment of packets $P1_1$ and $P2_1$ graphically indicates that in the example of collision C_1, both packets occupy the same frequency channel. Thus, collision C_1 represents an example where two different networks attempt to transmit packets during an overlapping time period and along the same channel.

[0008] Before proceeding with other types of packet collisions, an additional discussion is noteworthy with respect to a methodology which has been used to further reduce the likelihood and impact of packet collisions such as collision C_1. More particularly, this additional methodology is referred to in the art as listen-before-talk ("LBT"). In an LBT system, the system uses the hopping sequence described above, but prior to transmitting along a channel in the sequence the system monitors (or "listens") at the channel to determine if there is another packet already occupying that channel during the current time. Returning to packet $P1_1$ by way of example, if the second network employed LBT, then it would listen at the desired channel at which it intended to transmit $P2_1$ and would therefore detect the presence of packet $P1_1$. As a result, the second network would avoid collision C1 by not transmitting packet $P2_1$ at the desired frequency, but instead it would delay a random period and then proceed to the next designated channel of its hopping sequence. Next, the second network would listen at that next designated channel to again determine if that channel was occupied by a packet from another network, and if no packet was detected then the second network would transmit its packet; however, if this next designated channel also was occupied, then the second network would continue to examine additional channels in this same manner until a channel was detected without being occupied by a packet from another network, at which time the second network would transmit its packet along the now unoccupied channel. Given this process, however, note that a delay arises in LBT systems, where the amount of delay depends on the number of times that the LBT network is forced to listen, detect, and advance from an occupied channel, and then delay an additional random period to listen, detect, and transmit along an unoccupied channel.

[0009] While LBT as shown above reduces the possibility of collisions, it also has drawbacks. For example, LBT delays transmission by the network which was prepared to transmit along a channel but was prevented from doing so due to an already-transmitted packet in the desired channel. As another example, it adds an element of delay to each packet due to its listening aspect. Also, all the devices in an environment must utilize LBT to gain the most benefit (fairness) of the scheme. As still another example, some protocols (e.g., Bluetooth) utilized in the unlicensed bands do not support LBT, while such protocols may nonetheless provide other beneficial aspects and, thus, the choice to use such a protocol is a tradeoff in that other aspects are obtained without the availability of LBT.

[0010] Time t_2 in Figure 1 illustrates a second type of packet interference in connection with a collision C_2 occurring between a first network packet $P1_2$ and a second network packet $P2_2$. For collision C_2, the incumbent first network transmits packet $P1_2$ during a period including time t_2 and at a first channel, and thereafter the second network transmits packet $P2_2$ also during a period including time t_2 (i.e., the periods of the packets overlap). Packet $P2_2$ is transmitted at a second channel which, while different than the channel of packet $P1_2$, it is immediately adjacent the channel occupied by packet $P1_2$. Further in this regard, it is known in the art that while packets occupy a certain channel as shown by the vertical displacement of a packet in Figure 1, there is an additional tendency for a packet to provide slight interference or "splatter" into adjacent frequency channels. As a result of this effect, even though packets $P1_2$ and $P2_2$ occupy different channels, they are still in adjacent channels and, thus, they are close enough to one another in frequency such that the splatter effect causes a collision between the packets. Indeed, in some networks the filters used are relatively inexpensive and, as a result, the concept illustrated with packets $P1_2$ and $P2_2$ may also apply to next-adjacent channels, that is, to the channels that are one more channel away from the channels adjacent to the channel in which a packet is transmitted. Thus, collision C_2 represents an example where two different networks attempt to transmit packets during an overlapping time period and along adja-

cent (or next-adjacent) frequency channels. Here, if neither network uses LBT, then both packets $P1_2$ and $P2_2$ will require re-transmission due to the collision. If, however, the network that intended to transmit the second packet of the two uses LBT, then note first that LBT mechanisms are less likely to correctly discern an adjacent channel collision. However, if the LBT mechanism does recognize the potential adjacent channel collision, then the second packet is not transmitted along the channel represented by $P2_2$ and instead that packet is delayed. This delay, while diminishing the effective transmission of the second network, avoids any disturbance to the first already-existing packet. In the example of time t_2, therefore, if the second network uses LBT, then packet $P1_2$ will not be disturbed because the second network will move the transmission of packet $P2_2$ to a different channel.

[0011] Time t_4 in Figure 1 illustrates a third type of packet interference in connection with a collision C_4, which is comparable to collision C_2 except that for collision C_4 the networks transmit in opposite order. More particularly, for collision C_4, the second network first transmits a packet $P2_4$ and, thereafter, the first network transmits a packet $P1_4$. The duration of both of these packets overlaps time t_4, and again their channels are adjacent to one another rather than being the same channel. Nonetheless, the splatter effect again causes sufficient reach of each packet into the adjacent channel such that a collision occurs. Here, if neither network uses LBT, then both packets $P2_4$ and $P1_4$ require re-transmission due to the collision; if, however, the network transmitting the second packet in time (i.e., $P1_4$) of the two which would otherwise collide uses LBT, then only that packet is delayed and the first already-existing packet (i.e., $P2_4$) is not disturbed.

[0012] Time t_7 in Figure 1 illustrates a fourth type of packet interference in connection with a collision C_7, which is comparable to collision C_1 except that for collision C_7 the networks transmit in opposite order. More particularly, for collision C_7, the second network first transmits a packet $P2_7$ and, thereafter, the first network transmits a packet $P1_7$. The duration of both of these packets overlap time t_7 and their channels are the same. As a result, collision C_7 occurs (assuming the last network to transmit, which here is the first network, does not use LBT).

[0013] Figure 1 illustrates an additional type of potential interference by depicting a band of fixed interference FI. Fixed interference FI is intended to represent a non-network source of radio frequency transmission that remains at the same frequency for numerous time slots. Such fixed interference may arise from various devices, such as a leaking microwave oven by way of example. In any event, note at time t_5 that the second network transmits a packet $P2_5$, and the channel along which that packet is transmitted overlaps fixed interference FI. As a result, fixed interference FI interferes with packet $P2_5$, thereby requiring it to be re-transmitted. Once more, however, if the second network were to implement LBT, then assuming fixed interference FI were detected during the listening operation of the LBT, then packet $P2_5$ would not be transmitted so as to avoid the otherwise imminent interference. Lastly, while the example of packet $P2_5$ demonstrates a data collision where the packet uses the same channel as the fixed interference, note further that fixed interference also may disturb packets in a channel that is adjacent to the channel including the fixed interference. Once more, because some networks use relatively inexpensive filters, the fixed interference may corrupt packets which are either in a channel which is immediately adjacent to the fixed interference or which are in the next-adjacent channel (i.e., a channel which is next to the channel that is immediately adjacent to the fixed interference).

[0014] In view of the above, one skilled in the art should appreciate there are various opportunities for packet collision or packet interference to occur. Indeed, referring to Figure 1, the examples above demonstrate that an area may be described around each packet, where the packet is disturbed if another packet occurs within that area. Thus, this area, which may be perceived as a window or zone around the packet, is not only defined by the dimensions of the packet, but extends both before and after the packet by the width of another potentially-interfering packet, and extends above and below the packet channel through the height of at least the adjacent channel above and below the packet frequency channel. Still further, note that the packet sizes for both networks shown in Figure 1 are the same size by way of example; however, in some contexts, an incumbent network may use packets of different dimension (i.e., either in frequency and/or time) relative to the newly-entering network. In these cases, the packet size for the incumbent as well as the packet size for the newly-entering network, in addition to the window-affecting factors described above, all further define a two-dimensional area relative to a newly-entering packet in which interference may occur. Given the size of the two-dimensional area, therefore, there remains a possibility of packet disturbance even given the pseudo random nature of hopping spread spectrum RF communications.

[0015] As an additional consideration relative to avoiding packet collisions, it is further noted that the Federal Communications Commission ("FCC") imposes a restriction on the art in the Industrial Scientific Medical ("ISM") bands. Specifically, the FCC explicitly forbids independent networks to expressly cooperate in allocation of the wireless medium.

[0016] In view of the above, there arises a need to reduce the possibility of packet collision and interference, and preferably to do so in a manner that may be used with protocols that do not support LBT. The preferred embodiment addresses these goals, as is explored below. In addition, there arises a need to

achieve the above goals while complying the with the above-described FCC requirements. The preferred embodiments described below avoid these requirements by not requiring the newly entering network to have knowledge of or cooperation with the incumbent network.

[0017] In the preferred embodiment, there is a method for determining a frequency hopping sequence for a newly-entering network. The method comprises the step of scanning a plurality of frequency channels. For each of the plurality of frequency channels, the scanning step comprises detecting whether a signal exists on the channel and recording information corresponding to each channel on which a signal is detected. Finally, and responsive to the recorded information, the method forms the frequency hopping sequence. Other circuits, systems, and methods are also disclosed and claimed.

[0018] Specific embodiments of the invention will now be described, by way of example only, and with reference to the accompanying drawings, in which:

Figure 1 illustrates various packets transmitted by a first and second network and demonstrates potential collisions between such packets as well as interference from a band of fixed interference;

Figure 2 illustrates a flow chart of the preferred embodiment as implemented in a method performed by a network transceiver; and

Figure 3 illustrates a block diagram of a network transceiver operable to perform the method shown in Figure 2.

[0019] Figure 1 was described in the introductory description of this document and the reader is assumed familiar with that description.

[0020] Figure 2 illustrates a flow chart of a method 10 according to the preferred embodiment and for operating a wireless network so as to reduce the drawbacks described above in connection with the prior art. By way of introduction to this preferred embodiment, the following discussion demonstrates that by the conclusion of method 10 an improved hopping sequence is generated for a wireless network. The hopping sequence is improved in two respects. First, the hopping sequence is such that packets may be communicated according to it and results in a reduced amount of packet collisions as compared to a prior art non-LBT wireless frequency hopping system. Second, the hopping sequence is such that packets may be communicated according to it and results in a reduced incidence of conflict with fixed interference as compared to a prior art non-LBT wireless frequency hopping system. These benefits are illustrated in greater detail after the following detailed discussion of method 10. Finally, it should be noted that method 10 may be implemented in connection with various types of wireless networks as may be ascertained by one skilled in the art and as further addressed later. Additionally, such a person also may determine various different circuits and software implementations given the selected network, as is also explored later by way of example.

[0021] Method 10 begins with a step 12 where the wireless network begins the determination of a new hopping sequence to be used for intercommunications on the network (i.e., by all transmitters, receivers, and transceivers in the network). To facilitate the remaining discussion, the network which will use this new hopping sequence is referred to as the newly-entering network. This terminology is chosen because the newly-entering network's communications are new with respect to any one or more incumbent networks that already may be communicating along the frequency band to be used by the newly-entering network. In the preferred embodiment, step 12 occurs at network start-up, such as when a first transceiver of the newly-entering network is turned on or is otherwise initialized. Next, method 10 continues to step 14.

[0022] In step 14, a first frequency channel is selected for analysis. More particularly and as will become apparent given the remaining discussion of method 10, in the preferred embodiment each channel along which the newly-entering network may transmit is individually analyzed by method 10 at least once. Accordingly, step 14 operates so that a first one of these channels is selected to be analyzed. This selection may be implemented in various fashions, such as by assigning a unique and ascending number to each increasing frequency channel which is available to the newly-entering network, and then step 14 may operate by initializing a counter to the first assigned number. Other implementations may be ascertained by one skilled in the art. In any event, once a first channel is selected for analysis, method 10 continues to step 16.

[0023] In step 16, the channel selected by step 14 is scanned to determine if there is an existing signal in that channel. In the preferred embodiment, the known receive signal strength indicator ("RSSI") is used as the scan technique. Note that an existing signal may be detected in the scanned channel due to various events as illustrated earlier in connection with Figure 1. For example, an existing signal will be detected in step 16 if there is fixed interference in the scanned channel (or in a channel one or two adjacent channel locations from the scanned channel). As another example, an existing signal will be detected in step 16 if another network has transmitted a packet that, during the duration of the scan, is either in the scanned channel or in a channel that is adjacent the scanned channel. Each of these possibilities is responded to by one or more additional steps, as discussed below. Following the scan of step 16, method 10 continues to step 18.

[0024] Step 18 directs the flow of method 10 if the interference, if any, detected in step 16 is fixed interference. The determination of whether a particular detected interference is fixed interference (as opposed to packet interference) may be made in various fash-

ions. A simple approach is to wait on an occupied channel for a period of time which exceeds all known packet lengths (0.4 seconds by FCC part 15 rules). In a faster and preferred approach, the instance of a fixed interferer is determined by determining its occupied bandwidth, which is very small relative to data carrying modulated signals. More particularly, many scan circuits are available which can be configured according to the preferred embodiment to determine the bandwidth of a received signal by stepping through several sub-channels of the particular channel. In the process, the scanning circuit collects the RSSI as a function of each sub-channel and determines the half-power points, which is the bandwidth. Thus, once all sub-channels for the scanned channel are evaluated, and assuming that interference is detected on at least one of those sub-channels, then it may be further determined that the interference is fixed interference based on the bandwidth identified across all sub-channels. Specifically, fixed interference typically occupies only ten percent or less of the entire channel bandwidth; thus, if ten same-sized sub-channels are scanned for a given evaluated channel, and if the interference detected is only in one or two of those sub-channels, then the preferred embodiment determines that the detected interference is fixed interference; to the contrary, if interference is detected across most or all of those sub-channels, then the preferred embodiment determines that the detected interference is packet interference. In any event, if fixed interference is detected, then step 18 directs the flow to a step 20. To the contrary, if either no interference is detected, or if interference which is not fixed interference is detected, then method 10 continues from step 18 to step 22. Each of these alternative paths is described below.

[0025] In step 20, having been reached due to the detection of fixed interference existing in the scanned channel, method 10 records an indication of the time slot and channel in which the fixed interference was detected. The use of this information is detailed later. Thereafter, method 10 continues from step 20 to step 26, which is discussed following the discussion below concerning steps 22 and 24.

[0026] Step 22 directs the flow of method 10 if the potential interference, if any, detected in step 16 is interference from another packet being transmitted in the same, or an adjacent, channel as the channel scanned in step 16. In the preferred embodiment, the determination of whether a particular detected interference is packet interference (as opposed to fixed interference) is again made by measuring bandwidth which may then be compared with the known packet bandwidth, such as in connection with the sub-channel evaluation described above. If packet interference is detected in the scanned channel, then step 22 directs the flow to a step 24. To the contrary, if no interference was detected and step 22 is reached, then method 10 continues from step 22 to step 28. Each of these alternative paths is described below.

[0027] In step 24, the usage characteristics of the packet interference of the scanned channel are recorded. These characteristics preferably include the time slot and channel in which the packet was detected. In addition, when a potentially-interfering packet is detected in the scanned channel, there are two possible levels of information retrieval from that packet. As a first possibility, if the packet is detected in time to properly recover the header information from the packet, then that header information should include an indication of the hopping sequence of the incumbent network which transmitted the packet. For example, this indication may be by way of a seed which is used by the incumbent network which transmitted the packet and, more particularly, which is applied to a random sequence generator of the network to generate the incumbent network's frequency hopping sequence. In any event, the indication is stored by step 24 as a usage characteristic. As a second possibility, if the packet is not detected in time to properly recover its header information, then preferably a record is made of the time slot and frequency channel in which the packet was detected. Further in this regard, note that there is the chance that the existence of packet data in the scanned channel is detected, yet the actual data is relatively unintelligible. For example, if the incumbent system is not interoperable with the newly-entering system, then there is the possibility that the actual data from the incumbent's packet cannot be ascertained. However, even in this event, preferably the usage characteristics that are ascertained still include the time slot and frequency channel in which the packet was detected, and these characteristics are therefore preferably stored by step 24. Next, method 10 continues from step 24 to step 26.

[0028] The preceding demonstrates that step 26 may be reached when either fixed interference has been detected in the scanned (or an adjacent) channel, or when packet interference has been detected in the scanned (or an adjacent) channel, or indeed when no interference has been detected in the scanned channel. In all events, step 26 determines whether all channels that are available to the newly-entering network have been scanned. For example, in a contemporary 2.4 GHz ISM band wireless network, there are a minimum of 75 (of 83) required channels within the allowable ISM band. The incumbent transceiver produces between 2 and 1600 hops per second. Accordingly, applying step 26 to an ISM-based system will determine whether all 83 channels have been scanned. If not, method 10 continues to step 28 while, if all channels (from 75 to 83 in number) have been scanned, then method 10 proceeds to step 30.

[0029] Step 28 causes method 10 to prepare to repeat the above-described analysis with another channel that has not yet been scanned. This step is implemented in a manner compatible with the approach taken in step 14 to identify a first channel to be scanned.

For example, recall that earlier in connection with step 14 an approach was given where a counter was set to correspond to a first channel to be scanned. If this approach is selected, then step 28 may be implemented by incrementing this counter. In any event, once the network is properly prepared to evaluate another channel, method 10 returns from step 28 to step 16 and the above-described options are taken with respect to the next channel.

[0030] At some point given the return flow of method 10 described above, step 26 will determine that all channels available for transmission by the newly-entering network have been scanned; as noted above, at this point method 10 reaches step 30. Step 30 determines a hopping sequence for the newly-entering network given the information recorded by any previous occurrences of steps 20 and step 24. In other words, once step 30 is reached, if either or both of fixed or packet interference has been detected, then information has been stored regarding such interference and step 30 derives a favorable hopping sequence from that information. More particularly, given the detected information, step 30 generates a hopping sequence that will thereafter be used for transmission by the newly-entering network. This derived hopping sequence seeks to minimize the possibility that packets sent by the newly-entering network, and according to that hopping sequence, will incur interference given the already-existing interference as detected by earlier occurrences of step 16. In the preferred embodiment, the step 30 derivation of the hopping sequence is based first on determining, if possible, the hopping sequence of the incumbent network from previous information recorded in occurrences of step 24, and also in view of any recorded fixed interference recorded in occurrences of step 20. Thereafter, and as discussed later, the hopping sequence for the newly-entering network is derived. First, therefore, the preferred methods for determining the incumbent network's hopping sequence are described below. Second, the preferred methods for determining the newly-entering network's hopping sequence in view of the incumbent network's hopping sequence are also described below.

[0031] A first approach for determining the incumbent network hopping sequence is straightforward if an earlier occurrence of step 24 was able, as described above, to properly recover the header information from a detected incumbent network packet. In other words, recall that the header information includes an indication of the hopping sequence of the incumbent network which transmitted the packet. Thus, if such a header was properly decoded, then step 30 merely derives the incumbent network's hopping sequence from the indication in the packet header.

[0032] A second approach for determining the incumbent network's hopping sequence is achieved by extending the duration of step 16 to be large relative to the time that the incumbent network is expected to maintain a transmission along each of its available channels. For example, if the incumbent network is a Bluetooth network, then it is known that it will hop 1600 times a second, where for each hop only one packet is transmitted followed by another hop and packet transmission, and so forth. In addition, a Bluetooth network may hop among 83 different channels. Thus, where the incumbent network is a Bluetooth network, then the duration of step 16 may be set, by way of example, to one second. Given this duration, note that on average, for this one second duration which will therefore include 1600 hops to one of 83 different channels, then each different channel should be used approximately 19.27 times (i.e., 1600/83=19.27). As a result, during the one second scan duration in a given channel, approximately 19.27 packet detections should occur for that channel, and these detections are stored as the above-mentioned usage characteristics. Still further, this one second duration is then repeated for each different scanned channel, further enhancing the map to demonstrate approximately 19.27 detected packets for each channel scanned, along with the time intervals within the one second duration for different channel usages. Still further in the Bluetooth protocol, the hopping sequence repeats after 1600 hops; accordingly, given the mapped information described above, an accurate determination of the incumbent network's hopping sequence may be derived.

[0033] A third approach for determining the incumbent network's hopping sequence is achieved by shortening the duration of step 16 to be short relative to the time that the incumbent network is expected to maintain a transmission along one channel. More particularly, in this third approach each channel is scanned for a short enough duration so that all possibly used channels are scanned in a time period that is no greater than the time period that the incumbent network will continue to transmit along a single channel. Again using the example of an incumbent Bluetooth network, recall that it transmits successive packets along a maximum of 83 different channels. Accordingly, for the third approach the scan duration is equal to (or no greater than) 1/83 times the duration of a packet. By scanning in this manner, for 83 successively scanned channels, where each channel is scanned for only 1/83 of a packet duration, and assuming only a single Bluetooth incumbent network is transmitting, then only one channel during the scan should be found to be occupied by a packet (although adjacent channels may detect interference from the packet splatter). In this approach, note that step 26 of method 10 is modified so that the channels are scanned numerous times rather than just scanning all available channels once, so that eventually method 10 will detect usage in each of the available channels. Once more using the Bluetooth incumbent network by way of example, it is probable that after 1600 scans of each of the 83 channels (where each channel is scanned for 1/83 of the packet duration), then the entire incumbent network

hopping sequence should be mapped. This result follows since, during those 1600 scans, each channel will be shown to be used on average 19.27 times, and with the recorded information identifying when each such channel is used a map should result either demonstrating the incumbent network's hopping sequence, or from which the incumbent network's hopping sequence may be ascertained.

[0034] Once the incumbent network's hopping sequence is ascertained, such as by using any one of the three above-described preferred methods, then step 30 is completed by selecting a hopping sequence for the newly-entering network. In the preferred embodiment, the selected hopping sequence may be generated in one of two manners. In a first manner, the selected hopping sequence is identical to the incumbent network's hopping sequence for reasons more clear with respect to step 38 discussed below. In a second manner, each channel in the selected hopping sequence is selected so as to avoid the channels in the incumbent network's hopping sequence. In other words, the information ascertained from earlier occurrences of step 24 indicates each channel that is used according to the incumbent network's hopping sequence. Thus, in the second manner, for each time period the incumbent network will have used a channel, and in response to this information the newly-entering network's hopping sequence is created such that a different and non-adjacent channel will be used during that time period. Using either approach, the newly-entering network's hopping sequence has been created, and method 10 then proceeds from step 30 to step 32.

[0035] Step 32 modifies the newly-entering network's hopping sequence created in step 30 to avoid any channels detected to have fixed interference (i.e., as recorded in any earlier occurrence of step 20). More particularly, for each channel in the newly-entering network's hopping sequence that corresponds to a frequency in which there is fixed interference, then that channel in the sequence is not used and instead a replacement channel is selected. Further in this regard, note that in the preferred embodiment the replacement channel is selected from a rotation of channels in which there has not been a detection of fixed interference. The rotation also does not include either channels that were used in the previous time slot, or the following time slot, by the newly-entering network. Note that this rotation technique is preferred over using a same single alternative channel because the use of such a single channel may not provide sufficient randomness to satisfy the regulations of the FCC. Following step 32, method 10 continues to step 34.

[0036] Step 34 controls the method flow based on which of the two above-described techniques was implemented to choose the newly-entering network's hopping sequence, that is, whether it is the same as the incumbent network's hopping sequence (as modified by step 32) or whether it uses completely different channels than the incumbent network (as also modified by step 32). If the newly-entering network's hopping sequence is completely different, then method 10 continues to step 36 where the newly-entering network begins communicating according to its newly-developed hopping sequence. Alternatively, if the newly-entering network's hopping sequence is the same as the incumbent network's hopping sequence, then one additional step 38 is taken.

[0037] In step 38, method 10 waits for the incumbent network to complete its use of the first channel in the incumbent network's hopping sequence, and then step 38 waits at least one additional time slot thereafter. Next, the flow continues to step 36 where, as introduced above, the newly-entering network begins communicating according to its newly-developed hopping sequence. From the preceding, it should now be appreciated that if the newly-entering network uses essentially the same hopping sequence as the incumbent network, then the delay imposed by step 38 permits each packet transmitted by the newly-entering network to essentially occur at least two time slots later than a corresponding packet from the incumbent network and in the same channel. As a result, both networks use essentially the same hopping sequence (i.e., the newly-entering network hopping sequence being further modified so as to avoid fixed interference), but step 38 effectively causes the newly-entering network to lag in time behind the incumbent network. This lag, therefore, will prevent collisions between packets from the two networks since the incumbent network will always be at least two time slots ahead of the same channel usage by the newly-entering network.

[0038] Figure 3 illustrates a block diagram of a network transceiver 40 operable to perform method 10 shown in Figure 2, and which is shown here by way of example. In general, transceiver 40 includes three primary operational blocks, namely, a radio 42, a physical engine 44, and a media access control ("MAC") controller 46, all of which are standard in the wireless local area network ("LAN") art, and which are also described in the IEEE 802.11 standard for wireless LANs. In addition to the prior art functions of these blocks, however, they also are operable to perform the steps of method 10 from Figure 2. To the extent these blocks perform functions beyond those in method 10, such functions are ascertainable by one skilled in the art and are not detailed here. Further, note that the blocks of Figure 3 are shown by way of example to depict certain functions, while one skilled in the art may assign those functions to different blocks and also may select from various different circuits for accomplishing these functions. Also for sake of some completeness, transceiver 40 also includes an indication of a read only memory ("ROM") 48, a random access memory ("RAM") 50, and a host interface 52, as these additional aspects may well be expected by one skilled in the art to be included with a transceiver, although such extra devices need not

be detailed in connection with the operation of transceiver 40 relative to method 10. Lastly, the three primary blocks of transceiver 10, as well as the signals shown between those blocks, are discussed below in an order that parallels the steps of method 10 discussed earlier.

[0039] To commence method 10, MAC controller 46 asserts the Scan Command signal to physical engine 44. In response and to accomplish steps 16 through 24, physical engine 44 selects a channel and indicates the selected channel to radio 42 by the TX/RX Frequency signal. In response, radio 42 adjusts (e.g., its oscillator) to examine the signal at the indicated frequency and, recall in the preferred embodiment, an RSSI measurement is made at this frequency. Further in this regard, recall that it is discussed above that the preferred embodiment evaluates sub-channels within each selected scanned channel to determine if detected interference, if any, is either fixed interference or packet interference. Accordingly, physical engine 44 may indicate each such sub-channel to radio 42 via the Subchannel Scan signal or may indicate by that signal that sub-channels should be evaluated for the channel specified by the TX/RX Frequency signal; alternatively, radio 42 may be set up to evaluate a certain number of sub-channels (e.g., ten) for each channel indication it receives from physical engine 44. In any event, as radio 42 sweeps across sub-channels and determines corresponding RSSI measurements, it returns each measurement via the RSSI signal shown from radio 42 to physical engine 44. In response to the RSSI measurements, physical engine 44 makes the determinations of step 18 (i.e., whether interference is fixed) and step 22 (i.e., whether interference is from a packet), and potentially responds by taking the actions of steps 20 and 24, respectively. In addition, if RSSI is zero or negligible for a given scanned channel, then the preferred embodiment determines that there is no interference on that channel. In any event, once a channel is evaluated, physical engine 44 achieves step 28 by adjusting the TX/RX Frequency signal to the next channel (or sub-channel within the next channel) to be scanned, and the process repeats for all channels. Finally, once all channels are selected, the results of all detected interference are reported by physical engine 44 to MAC controller 46 via the Scan Results signal.

[0040] Once MAC controller 46 receives the Scan Results signal, it performs steps 30 and 32 directed to creating and modifying a new hopping sequence for the newly-entering network. Further, once this new hopping sequence is finalized, then MAC controller 46 communicates it to physical engine 44 via the Hop Sequence signal, and MAC controller 46 then instructs MAC controller 46 to actually begin hopping (i.e., transmitting per the new hop sequence) by asserting the Hop Control signal. This latter aspect, therefore, may be asserted to accommodate the delay aspect of step 38 if applicable.

[0041] From the above, it may be appreciated that the preferred embodiments provide various alternatives whereby a newly-entering network first scans the frequency channels along which it may transmit and in response to existing signals on those channels a hopping sequence is derived for the newly-entering network. The hopping sequence for the newly-entering network provides numerous advantages over the prior art. For example, packets transmitted according to the newly-entering network's derived hopping sequence are considerably less like to incur interference as opposed to a non-LBT prior art wireless network. Further in this regard, therefore, the preferred embodiments may be used with Bluetooth or other non-LBT protocols, thereby gaining access to the features of those protocols, while still having a reduced incidence of packet interference even without the LBT functionality. Indeed, this benefit is particularly useful given that Bluetooth may well become a very prevalent protocol and, for this reason, the preferred embodiment specifically contemplates a Bluetooth implementation. As another example, the preferred method does not require a delay associated with each individual packet transmission as does an LBT architecture. As still another example, recall that the FCC imposes a regulation on wireless networks in that they are not permitted to explicitly coordinate with one another, and the preferred embodiment satisfies this regulation while still achieving a reduced incidence of packet interference. As still another example, while the preferred embodiment has been discussed primarily in connection with the Bluetooth protocol, such discussion is by way of example and, thus, the above teachings may be applied to other systems as well (e.g., IEEE 802.11) and combination of several Bluetooth and 802.11 frequency hopping devices. Still further, the preferred embodiment may be used in numerous different wireless band systems (e.g., the ISM band, and others). Consequently, while the present embodiments have been described in detail, the preceding further demonstrates that various substitutions, modifications or alterations could be made to the descriptions set forth above without departing from the inventive scope which is defined by the following claims.

[0042] An optional embodiment comprises a computing device such as a general purpose microprocessor or digital signal processor, configured to operate a transceiver in accordance with the flowchart illustrated in Figure 2. The programmable logic device is configured by means of a computer program to perform the steps of the flowchart of Figure 2, in cooperation with the operational elements of the transceiver.

[0043] The computer program may be carried or stored in any suitable carrier medium, such as volatile or non-volatile solid state memory, resident in the transceiver or associated circuitry. Additionally, the computer program may be carried on a magnetic disc or tape, or over a telecommunications medium such as an optical frequency or radio frequency carrier signal, for delivery

to the solid state memory in the transceiver, for example.

[0044] The scope of the present disclosure includes any novel feature or combination of features disclosed therein either explicitly or implicitly or any generalisation thereof irrespective of whether or not it relates to the claimed invention or mitigates any or all of the problems addressed by the present invention. The applicant hereby gives notice that new claims may be formulated to such features during the prosecution of this application or of any such further application derived therefrom. In particular, with reference to the appended claims, features from dependent claims may be combined with those of the independent claims and features from respective independent claims may be combined in any appropriate manner and not merely in the specific combinations enumerated in the claims.

Claims

1. A method for determining a frequency hopping sequence for a newly-entering network, comprising the steps of:

    scanning a plurality of frequency channels, comprising for each of the plurality of frequency channels the steps of:
    detecting whether a signal exists on the channel; and
    recording information corresponding to each channel on which a signal is detected; and
    responsive to the information, forming the frequency hopping sequence.

2. The method of claim 1 wherein the detecting step comprises detecting whether a packet signal exists on the channel on which the signal is detected.

3. The method of claim 2 wherein the packet signal exists on the channel in response to a packet communicated by an incumbent network along the channel on which the signal is detected.

4. The method of claim 3:
wherein the detecting step comprises detecting an indication of a hopping sequence for the incumbent network and corresponding to the packet communicated by the incumbent network; and
wherein the recording step comprises recording the indication.

5. The method of any preceding claim, wherein the recording step comprises:

    recording an identifier of the channel on which the signal is detected; and
    recording a time indication corresponding to when the signal is detected.

6. The method of any of claims 1 to 3, wherein the detecting step further comprises detecting whether a fixed interference signal exists on the channel on which the signal is detected.

7. The method of claim 6, wherein the recording step comprises recording an identifier of the channel on which the fixed interference signal is detected.

8. The method of claim 6 or 7, wherein each of the steps of detecting whether a packet signal exists and detecting whether a fixed interference signal exists is responsive to a bandwidth of the signal on the channel.

9. The method of claim 6 or 7, wherein each of the steps of detecting whether a packet signal exists and detecting whether a fixed interference signal exists is responsive to a scan of a plurality of subchannels of the channel.

10. The method of claim 6 or 7:
wherein each packet communicated by the incumbent network has a known maximum duration; and
wherein the step of detecting whether a fixed interference signal exists is responsive to scanning each of the plurality of frequency channels for a period of time which exceeds the maximum duration.

11. The method of claim 2, wherein the packet signal exists on the channel in response to one of either:

    a packet communicated by an incumbent network along the channel on which the signal is detected; and
    a packet communicated by an incumbent network along a channel adjacent to the channel on which the signal is detected.

12. The method of claim 1:
wherein the detecting step detects packet signals in response to packets communicated along the plurality of frequency channels by an incumbent network having an incumbent network hopping sequence; and
wherein the step of forming the frequency hopping sequence for the newly-entering network comprises forming the hopping sequence equal to the incumbent network hopping sequence.

13. The method of claim 12, and further comprising the steps of:

    waiting until the incumbent network transmits a first packet along a first channel corresponding to a first channel in the incumbent network hopping sequence; and

after the waiting step, transmitting a packet with the newly-entering network according to the hopping sequence for the newly-entering network.

14. The method of claim 1:
wherein the detecting step detects packet signals in response to packets communicated along the plurality of frequency channels by an incumbent network having an incumbent network hopping sequence;
wherein the detecting step detects signals in response to fixed interference along at least one of the plurality of frequency channels; and
wherein the step of forming the frequency hopping sequence for the newly-entering network comprises:

forming a first hopping sequence equal to the incumbent network hopping sequence; and
forming the frequency hopping sequence for the newly-entering network by modifying the first hopping sequence to not include any one of the plurality of channels along which fixed interference is detected.

15. The method of claim 14, wherein the modifying step comprises selecting an alternative channel from a rotation of channels such that the selected alternative channel is used in the frequency hopping sequence for the newly-entering network in place of one of the plurality of channels along which fixed interference is detected.

16. The method of claim 15, wherein the rotation of channels comprise a plurality of interference-free channels in which the detecting step has not detected a signal existing on each of the interference-free channels.

17. The method of any one of claims 1 to 15:
wherein the scanning step is operable to identify packet signals in response to a hopping sequence of an incumbent network;
wherein the hopping sequence of the incumbent network consists of an integer number N of different channels along which the incumbent network may transmit packets;
wherein the step of scanning a plurality of frequency channels comprises scanning each of the plurality of frequency channels multiple times; and
wherein for each of the multiple times each of the plurality of frequency channels is scanned for a period no greater than a ratio of one over the integer N.

18. The method of any one of claims 1-15:
wherein the scanning step is operable to identify packet signals in response to a hopping sequence of an incumbent network;
wherein the hopping sequence of the incumbent network consists of an integer number M of sequence channels over which the incumbent network is operable to transmit packets before repeating the hopping sequence of the incumbent network; and
wherein the step of scanning a plurality of frequency channels comprises scanning each of the plurality of frequency channels for a period at least equal to a time required by the incumbent network to transmit packets along the integer number M of sequence channels.

19. A computer program for configuring a computing device to implement and/or control a communications device to carry out the steps of any one of claims 1 to 18.

20. A computer program carrier medium carrying a computer program according to claim 19.

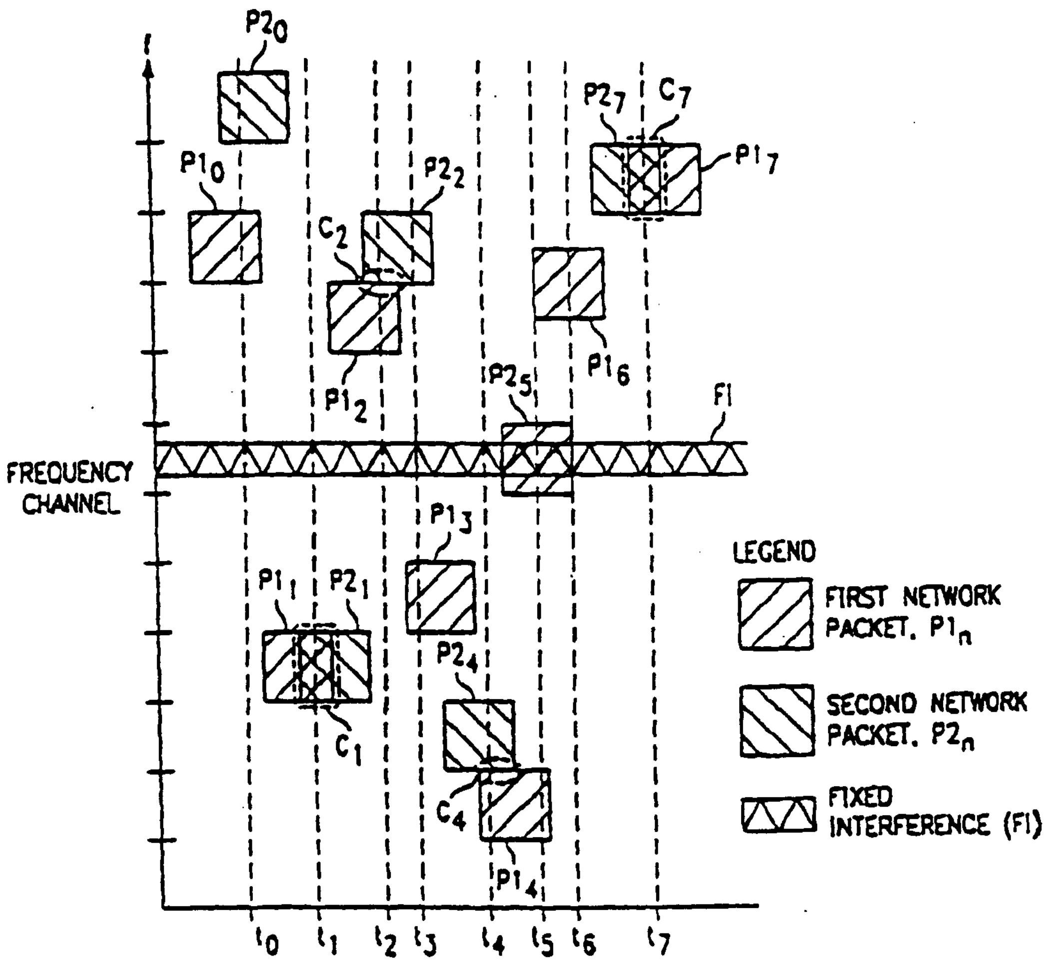

f
FREQUENCY CHANNEL
P2₀
P1₀
C₂
P2₂
P1₂
P2₅
P1₆
P2₇
C₇
P1₇
FI
P1₃
P1₁
P2₁
C₁
P2₄
C₄
P1₄
t₀ t₁ t₂ t₃ t₄ t₅ t₆ t₇
LEGEND
FIRST NETWORK PACKET, P1ₙ
SECOND NETWORK PACKET, P2ₙ
FIXED INTERFERENCE (FI)

FIG. 1

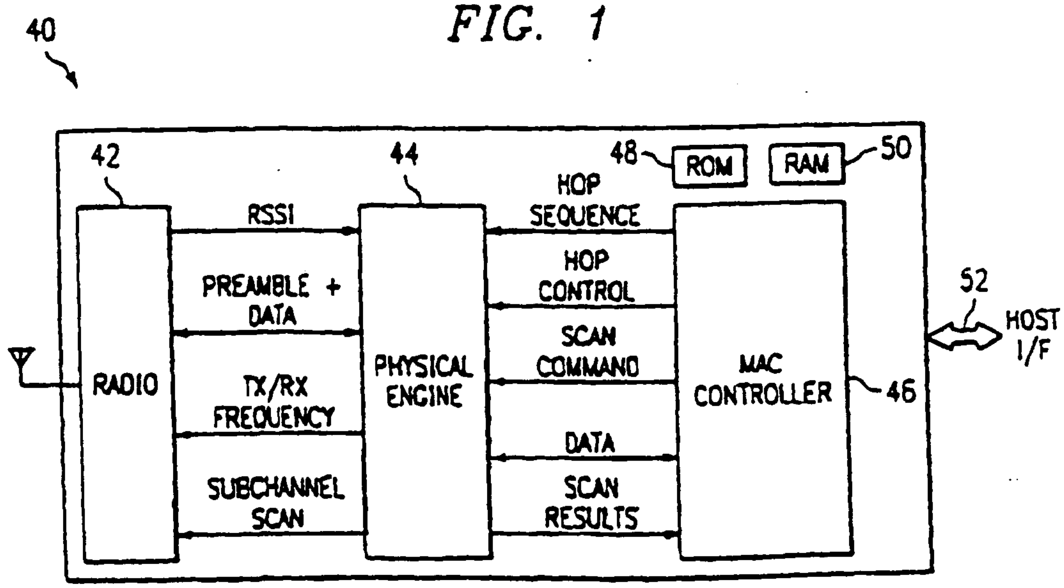
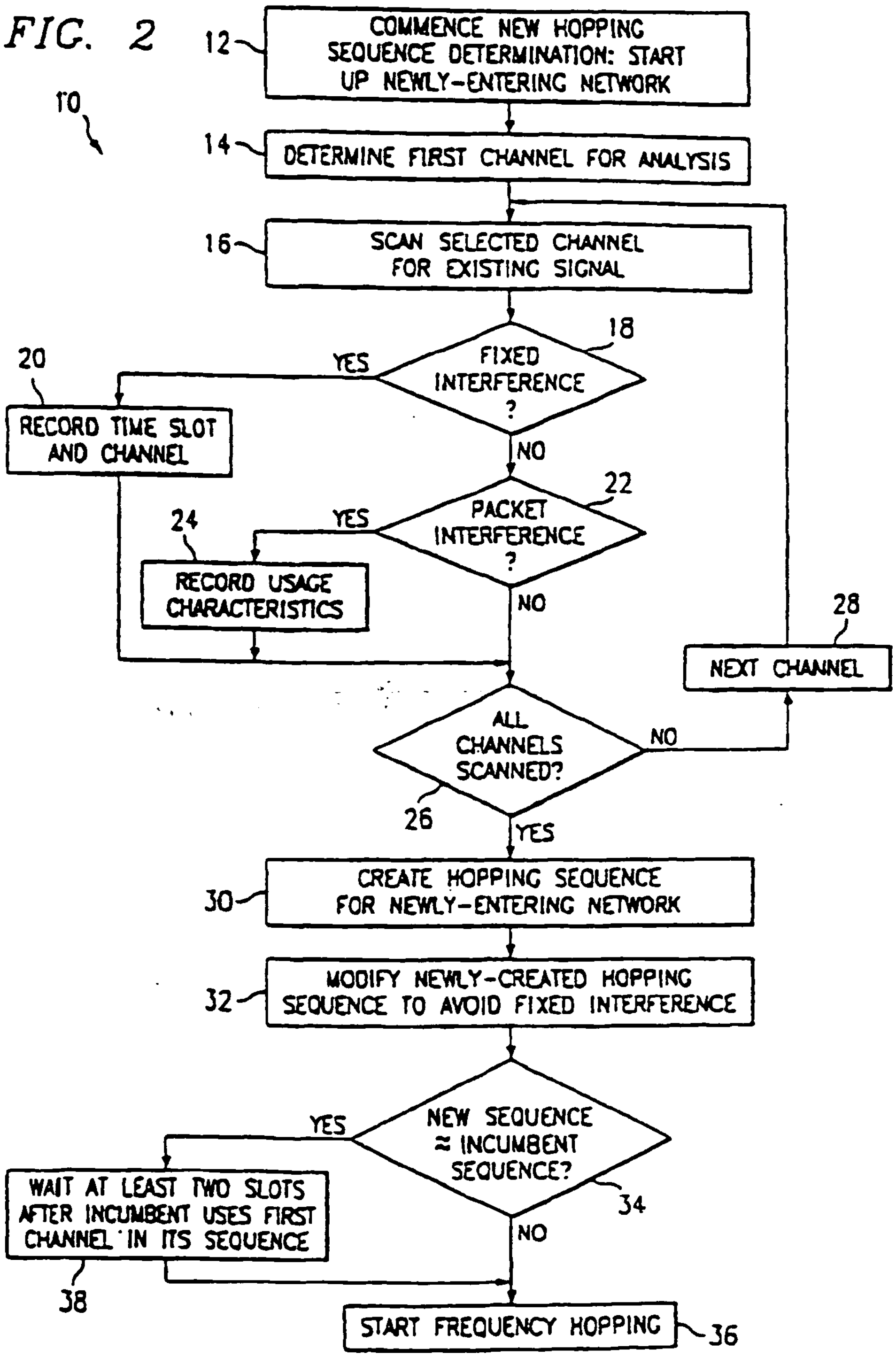

40
42
44
48
ROM
RAM
50
RADIO
RSSI
PREAMBLE + DATA
TX/RX FREQUENCY
SUBCHANNEL SCAN
PHYSICAL ENGINE
HOP SEQUENCE
HOP CONTROL
SCAN COMMAND
DATA
SCAN RESULTS
MAC CONTROLLER
46
52
HOST I/F

FIG. 3

FIG. 2


10
12
COMMENCE NEW HOPPING SEQUENCE DETERMINATION: START UP NEWLY-ENTERING NETWORK
14
DETERMINE FIRST CHANNEL FOR ANALYSIS
16
SCAN SELECTED CHANNEL FOR EXISTING SIGNAL
18
FIXED INTERFERENCE ?
YES
NO
20
RECORD TIME SLOT AND CHANNEL
22
PACKET INTERFERENCE ?
YES
NO
24
RECORD USAGE CHARACTERISTICS
28
NEXT CHANNEL
ALL CHANNELS SCANNED?
NO
26
YES
CREATE HOPPING SEQUENCE FOR NEWLY-ENTERING NETWORK
30
MODIFY NEWLY-CREATED HOPPING SEQUENCE TO AVOID FIXED INTERFERENCE
32
NEW SEQUENCE ≈ INCUMBENT SEQUENCE?
YES
34
NO
WAIT AT LEAST TWO SLOTS AFTER INCUMBENT USES FIRST CHANNEL IN ITS SEQUENCE
38
START FREQUENCY HOPPING
36